Honeywell

TotalPlant™ Systems Security

Jim Weeldreyer

Honeywell Automation and Control Solutions

jim.weeldreyer@honeywell.com

September 10, 2001

ISA 2001, Houston

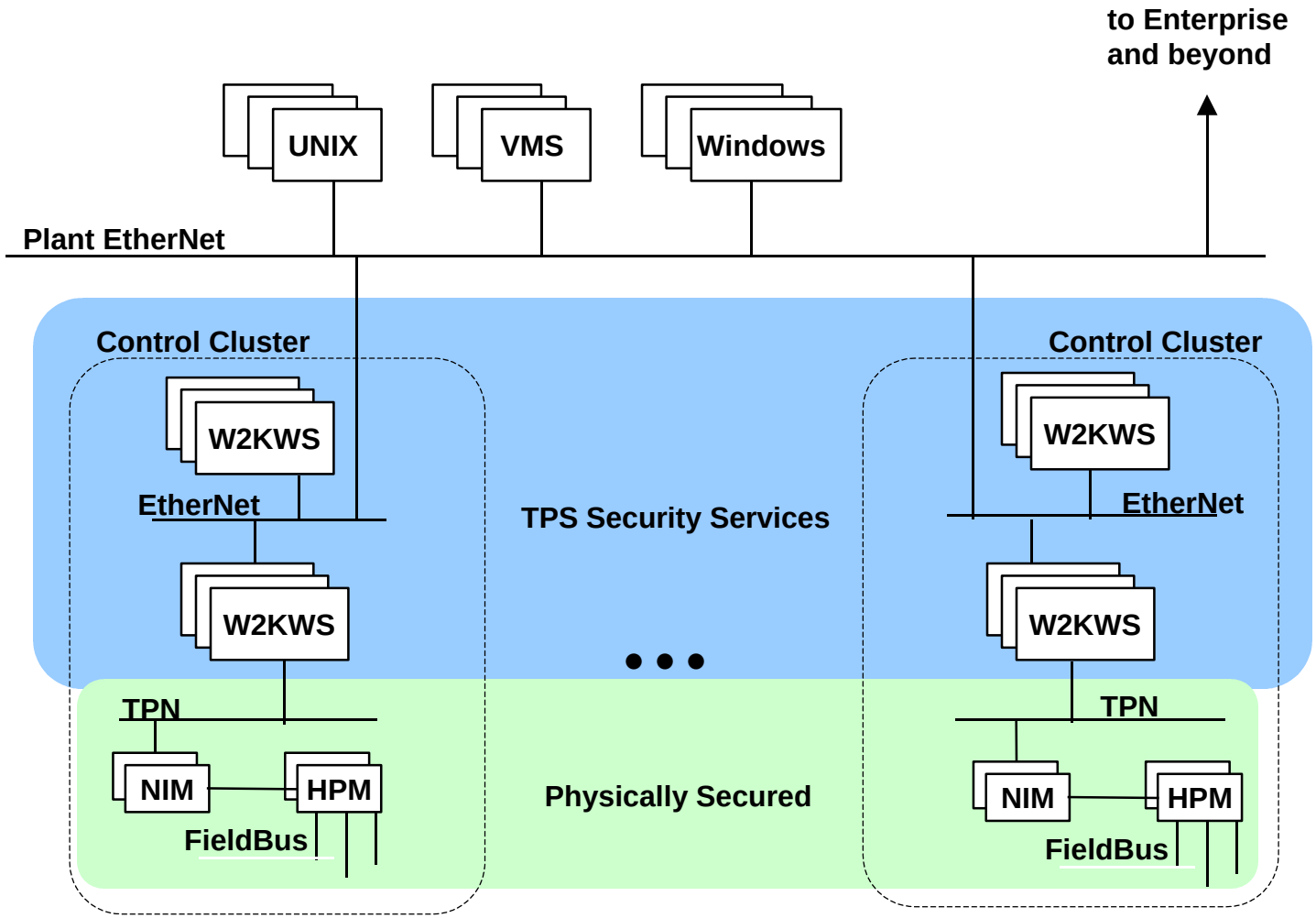
Topics

- Scope
- Computing Environment
- Functional Description
- Security Model Description
- Integration with Other Systems
- Response to EPRI Vulnerabilities
- Summary

Scope

- **Honeywell TotalPlant™ Systems (TPS)**
  - **Promote consistent implementation of security functions**
- **Security threats**
  - **Unauthorized access over open networks**
  - **Unauthorized access by local personnel**
  - **Primary vulnerabilities are in the area of open access through Windows 2000**

Computing Environment

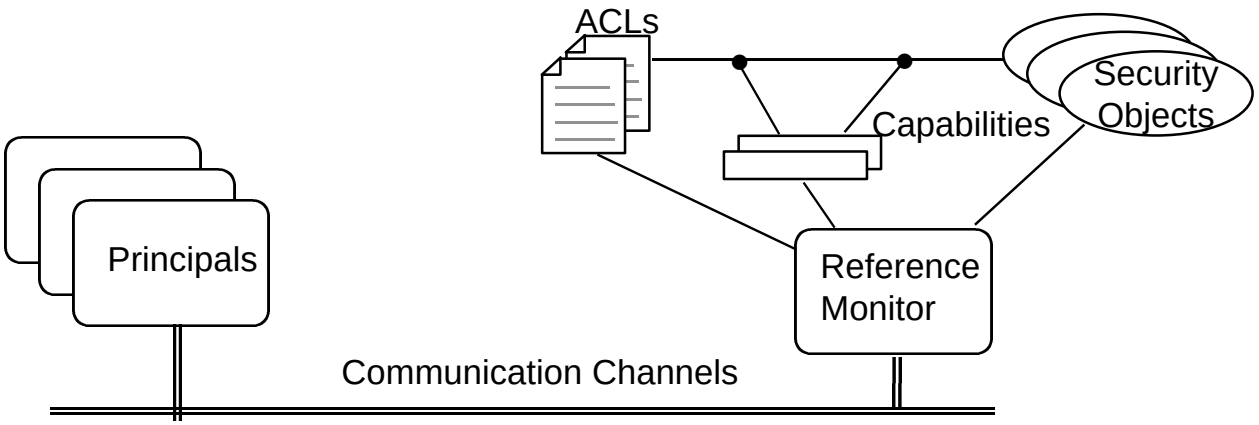


W2KWS = Windows 2000 Work Station; NIM = Network Interface Module;
HPM = High performance Process Manager; TPM = TotalPlant Network

Functional Description

- **Majority of security implementation is on the Windows 2000 platforms, with minimal impact on controllers**
- **Leverage Windows 2000 security mechanisms**
- **Augment Windows 2000 mechanisms only where necessary**
  - **Ensure that augmentations are well integrated with Windows 2000**
- **Control accesses from non-Windows platforms using a combination of Windows 2000 and Internet facilities provided by Microsoft**

Security Reference Model



Principal: An active entity which can make a request to perform an operation on a security object, e.g. a user, a server process, a computer system. Within TPS, a Principal is identified by its Windows 2000 Access Token.

Security Object: An entity to which access is controlled, e.g. a file, a database element, a computer system, a TPS database object.

Capability: A capability represents an access right to those security objects with which it is associated. If a principal has permission to acquire a capability, it has the access right to the associated security objects, represented by the capability. Note: a capability is itself a security object. Can be viewed as a "role".

ACL: (Access Control List) is associated with exactly one capability or other security object, and contains a list of principals (or principal groups) which have access to that capability/security object, together with their access rights. TPS utilizes Windows ACLs.

Reference Monitor: A principal which is associated with one or more security objects and restricts access to those security objects to only those principals possessing the required access rights, as determined by the associated ACL or capabilities. Within TPS, the Windows Reference Monitor controls access to standard Windows objects, and TPS Reference monitors control access to TPS objects, e.g. the TPS process database.

Communication Channel: An information path among two or more principals.

Integration of Foreign and Legacy Systems

- **As servers:**
  - **Integrated via OPC**
    - Implementation maps between TPS and the foreign system security mechanisms (if available)
    - Implementation may provide its own TPS security layer for the foreign system
  - **Example is the TPN**
    - Key level (role) is mapped to a capability on the Windows 2000 side
    - The TPN continues to manage its own security
- **As clients:**
  - **Integrated via Windows 2000 and Internet security mechanisms**
  - **Client principals have access credentials as recognized by Windows 2000**
  - **Windows 2000 and TPS reference monitors make authorization decisions based on these credentials**

EPRI Security Vulnerabilities

- **Media Security**
  - **Outside scope of TPS**
- **Protocol Security**
  - **Ethernet TCP/IP: Windows 2000 authentication available**
  - **Others: Outside scope of TPS**
- **Database Security**
  - **DCS, History: Role based security, based on Windows Access Token**
  - **Third party database**
    - As server: Vendor provided
    - As TPS client: Based on Windows Access Token (of account it's running under)
  - **Web Server: Provided by the server developer**
  - **Direct Access from outside systems: Provided by host application**
  - **Operator/Engineer Workstation: Windows 2000 login**
  - **Remote Access Modems**
    - Remote access to operator stations for service and diagnostics: Operator controls access
- **Application Security**
  - **As TPS Client: Based on Windows Access Token (of account it's running under)**
  - **As server: Vendor provided**

Summary

- **The TPS security approach:**
  - **Integrates with Windows 2000 security mechanisms, and leverages them extensively**
  - **Extends Windows 2000 mechanisms to address requirements specific to control systems**